

THIS DISPOSITION IS
NOT CITABLE AS
PRECEDENT OF THE
TTAB

Mailed:
29 September 2004
AD

UNITED STATES PATENT AND TRADEMARK OFFICE

Trademark Trial and Appeal Board

In re Hypercom Corporation

Serial No. 76424261

Laura J. Zemah of Snell & Wilmer, LLP for Hypercom Corporation.

Caroline Fong Weimer, Trademark Examining Attorney, Law Office 115 (Tom Vlcek, Managing Attorney).

Before Simms, Rogers, and Drost, Administrative Trademark Judges.

Opinion by Drost, Administrative Trademark Judge:

On June 24, 2002, applicant (Hypercom Corporation) applied to register the mark SECURITY BIOMETRICS, in typed form, on the Principal Register for "computer hardware and software for use with identification systems and point-of-sale transaction systems for identifying and verifying

identity of individuals using fingerprint, voice, eye and facial feature data," in International Class 9.¹

The examining attorney refused to register applicant's mark on the ground that the mark was merely descriptive under Section 2(e)(1) of the Trademark Act, 15 U.S.C. § 1052(e)(1). The examining attorney argues (Brief at 3) that the "use of biometric data within the system ... provides a means of secure authentication" and that the applicant "has combined the descriptive words for their descriptive meaning." Applicant contends (Reply Brief at 2-3) that its goods are "not a fingerprinting system but rather a positive identification system that uses some aspects of the fingerprint to create a natural signature to protect consumers and eliminate fraud." Applicant goes on to argue (Reply Brief at 3) that its mark is not descriptive of the identified goods because they "do not use fingerprint images to verify identification but instead [use] a vector."

After the examining attorney made the refusal final, applicant appealed to this board.

A mark is merely descriptive if it immediately describes the ingredients, qualities, or characteristics

¹ Serial No. 76424261 was based on a allegation of a bona fide intention to use the mark in commerce.

of the goods or services or if it conveys information regarding a function, purpose, or use of the goods or services. In re Abcor Development Corp., 588 F.2d 811, 200 USPQ 215, 217 (CCPA 1978). See also In re MBNA America Bank N.A., 340 F.3d 1328, 67 USPQ2d 1778, 1780 (Fed. Cir. 2003) (A "mark is merely descriptive if the ultimate consumers immediately associate it with a quality or characteristic of the product or service"); In re Nett Designs, 236 F.3d 1339, 57 USPQ2d 1564, 1566 (Fed. Cir. 2001).

To be merely descriptive, a term need only describe a single significant quality or property of the goods. In re Gyulay, 820 F.2d 1216, 3 USPQ2d 1009, 1009 (Fed. Cir. 1987); Meehanite Metal Corp. v. International Nickel Co., 262 F.2d 806, 120 USPQ 293, 294 (CCPA 1959). We look at the mark in relation to the goods or services, and not in the abstract, when we consider whether the mark is descriptive. Abcor, 200 USPQ at 218.

First, we examine the evidence concerning the meaning of the terms "biometrics" and "security," when they would be used with applicant's goods.

Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and

irises, voice patterns, facial patterns and hand measurements, especially for authentication purposes.

Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scanned image into digital form, and wherever the data is to be analyzed, a database that stores biometric data for comparison with previous records.

Fingerprint, facial, or other biometric data can be placed on a smartcard and users can present both the smartcard and their fingerprints or faces to merchants, banks, or telephones for an extra degree of authentication.

SearchSecurity.com Definitions.

Recently the term "Biometrics" has been used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.

Biometrics Journal, "Definition of Biometrics."

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are: face, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent... Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric Consortium, "An Introduction to Biometrics."

Applicant's goods will be used with identification systems for identifying and verifying the identity of individuals using fingerprint, voice, eye, and facial feature data. Similar to the excerpts on biometrics above, applicant admits that its product would be designed "to protect consumers and eliminate fraud." Reply Brief at 3. As the evidence above indicates, fingerprint, eye, voice, and facial data are the subject matter of biometrics. The use of this data is needed for "highly secure identification." Applicant also admits that its "hardware and software scan the fingerprint, extract a vector, and discard the fingerprint image." Reply Brief at 2. While applicant's identification of goods is not limited to this use, even applicant's argument indicates that biometric data (fingerprint information) is used to provide positive identification and verification. The record certainly supports the conclusion that hardware and software that use fingerprint, voice, eye, and facial feature data for identifying and verifying the identity of individuals are using biometric information. Therefore, the term "Biometrics" would describe applicant's goods.

The other term in applicant's mark is the word "Security." This term also would have descriptive significance when used with applicant's goods. Biometric

information provides solutions to "security breaches and transaction fraud." According to the record, network security infrastructures and secure electronic banking are already benefiting from this technology. Applicant has submitted a definition of "security" that, inter alia, includes the following: "Measures taken to guard against espionage or sabotage, crime, attack or escape." Response dated May 5, 2003. The use of biometric information would qualify as a measure to guard against sabotage, crime, or attack upon information in a database. Therefore, the term "security" describes hardware and software used to verify the identity of individuals to prevent unauthorized access to data and thereby keep the information secure.

However, despite the descriptiveness of the individual terms, it is the mark as a whole that we must ultimately consider in our determination of whether applicant's mark is merely descriptive. We emphasize that the issue of whether the mark is descriptive is viewed from the perspective of the potential purchasers of applicant's software and not necessarily from those who input their personal information for verification. We find that, to the potential purchasers of applicant's software, there is nothing incongruous or vague about the term SECURITY BIOMETRICS for applicant's identified

computer hardware and software. The mark would simply describe the fact that applicant's goods use biometric data to improve or enhance security. For example, the information of record contains a reference to another article entitled "Biometric Management and Security for the Financial Services." See *Biometric Consortium*.

Finally, we note that applicant's goods are identified as hardware and software used with point-of sale transaction systems that are used for identifying and verifying the identity of individuals using fingerprint, voice, eye and facial features. Therefore, while applicant argues that "no fingerprint images are transmitted or stored," this is not significant because nothing in applicant's identification of goods requires the transmission of the actual fingerprints themselves as opposed to information culled from the fingerprints. In addition, applicant's goods are not limited to transmitting information on fingerprints. They obviously include using voice, eye, and facial features along with fingerprints for identifying and verifying individuals. As discussed previously, this data would be biometric information.

We have no doubts that when prospective purchasers of applicant's software encounter the term SECURITY

BIOMETRICS, the term would immediately describe applicant's software that uses biometric information to verify the identity of individuals. Therefore, we affirm the refusal to register.

Decision: The refusal to register under Section 2(e)(1) of the Trademark Act is affirmed.